

British Data Breach Caused by Upset Employee Provides Lesson for Companies Worldwide

November 4, 2015 — After being disciplined by his employer, Morrison's, for using the company's mail room to run his shop on eBay, Andrew Skelton decided to retaliate. So, he created a data breach that leaked the personally identifiable information on 100,000 employees of the British based supermarket chain. Skelton has since been tried and convicted. He is now serving an 8 year prison term. But the nightmare for Morrison's is far from over. The company is now being sued by affected employees.

[Tweet](#)

```
(function() {
  var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
  s.type = 'text/javascript';
  s.src = 'http://widgets.digg.com/buttons.js';
  s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
  po.src = 'https://apis.google.com/js/plusone.js';
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

Skelton was a Senior Auditor in Morrison's headquarters. His position gave him access to a wide variety of confidential company information including the company's employee database.

After his conviction, a group of nearly 2,000 employees filed suit against the company for not adequately protecting their personal information. A British court has now given the group approval to move forward with the suit. The plaintiffs in the case were also given a green light to get more of Morrison's employees involved in the suit.

While British and European Union privacy laws are considerably stronger than those in the United States, this incident provides an object lesson for companies worldwide. A poll conducted earlier this year by Sans Institute found that 40% of businesses have no plans in place to deal with data breaches caused maliciously by employees.

There is very little doubt that a data breach of this type in the United States would lead to a similar lawsuit. Regardless of the outcome of such a suit, the bad publicity generated as a result of the suit could prove extremely expensive to a defendant corporation.

Companies need to have policies in place to limit the access to employee data, to store such data in encrypted form, and to change sign-on credentials for such access on a regular basis. Given what happened at Morrison's, companies should seriously consider changing those sign-on credentials prior to taking any disciplinary action against an employee with this type of access.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click [here](#). Registration is easy and free.

Follow me on Twitter:

Follow ACCESS